代號：30160
頁次：1－1

115年公務人員特種考試警察人員、一般警察人員、國家安全局國家安全情報人員及移民行政人員考試試題

考 試 別：一般警察人員考試
等　　別：二等考試
類科組別：刑事警察人員數位鑑識組
科　　目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）
考試時間：2 小時　　座號：＿＿＿＿＿＿

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、請回答下列有關雜湊函數與生日攻擊之問題：
㈠雜湊函數（Cryptographic Hash Functions）有那些應用？一個理想的 Cryptographic Hash Function 必須具備那些關鍵特性？說明其理由並舉例。（10 分）
㈡詳細說明什麼是生日攻擊（Birthday Attack）？Birthday Attack 對於網路資訊應用帶來什麼資安威脅？請舉例說明之。（15 分）

二、請回答下列有關網路安全偵察以及協定攻擊之問題：
㈠何謂網路安全偵察（Cybersecurity Reconnaissance）？被動偵查與主動偵查之差異為何？請詳細說明並舉例。（10 分）
㈡何謂網路協定攻擊（Network Protocol Attack）？網路協定攻擊有那些常見的攻擊方法？舉例說明有那些防禦策略？（15 分）

三、使用公共 Wi-Fi 傳送機敏資料會帶來資安風險，例如：遭受邪惡孿生（Evil Twin）攻擊。
㈠何謂 Evil Twin 攻擊？Evil Twin 攻擊有那些資安威脅？舉例說明之。（10 分）
㈡何謂保護無線網路的安全協定（Wi-Fi Protected Access, WPA）？WPA 及其相關的標準實現了那三項安全特性，以解決使用網路遭遇到的安全問題？詳細說明之。（15 分）

四、資安事件之處理與應變，需要遵循國家相關的法規，以及國際標準。
㈠有關資安事件之通報與應變，我國是依據那部法律，訂定什麼辦法加以規範？並說明其對於資安事件如何分級，以及通報內容應包括之項目。（10 分）
㈡ ISO/IEC 27035 事件管理生命週期（Incident Management Lifecycle）的目的為何？透過遵循事件管理生命週期會有那些優勢？（15 分）